REMARKS

The Office Action dated October 5, 2004, has been carefully reviewed and the following remarks are submitted in response thereto. Claims 1, 3-12, 14, 15, and 17 are pending in the application.

The rejection of claims 1, 3-7, 9-12, 14, 15, and 17 under 35 USC 102(e) as being unpatentable over Buck et al is respectfully traversed. Claims 1, 12, and 16 recite that if a respective firewall is in place between the called user and the internetwork, then it is detected whether a respective firewall is in place between the calling user and the internetwork. If a respective firewall is not in place between the calling user and the internetwork, then the calling user's respective global address is transmitted to the called user and the called user establishes a network session for the connection with the calling user by transmitting to the calling user's respective global address. Thus, in view of the discovered firewall configuration, the present invention dynamically reverses the roles of the users' computers for establishing the direct (peer to peer) network session.

The recited limitations are neither shown nor suggested by Buck. Buck does not and cannot establish a network session directly between the calling user and the called user unless no NAT firewall is in place at the called end. Buck concerns the use of a gateway to act as a proxy to echo network packets between users (see Figures 5-12 and paragraph 0057, for example), with the gateway performing re-packaging of packets between TCP and UDP protocols in order to pass through certain firewalls. Bypassing of the gateway server in Buck is only possible when the firewalls present do not interfere with the UDP protocol (see paragraph 0055) and when the firewall does not perform network address translation (see the second note in Table 1).

Obviously, a direct connection is always possible when neither user is behind any kind of firewall. The language quoted on page 2 of the final rejection shows merely that the gateway server in Buck et al can be bypassed if message packets are in a format that is not blocked by existing firewalls at either end. The type of firewall discussed in the quoted language is the type that prohibits certain packet

formats. The quoted language does not suggest that Buck et al claims to be able to circumvent any network address translation that occurs at the recipient end, and in fact Buck et al cannot handle a direct connection between users if the recipient has a NAT firewall. That is why the note to Cases 2 and 5 in Table 1 states that the gateway server is still needed in the presence of a NAT firewall. In Cases 2 and 5, the sending and receiving packet formats are compatible for both directions of communication. Nevertheless, the system in Buck et al still needs the gateway server because it offers no solution to the problem of a NAT firewall implemented by the called user.

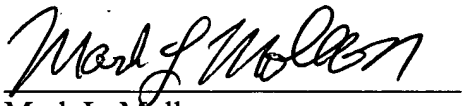
The present invention overcomes the problem of NAT being performed in the called user's firewall by having the called user's computer establish the network session. Buck is incapable of doing so. Claims 1, 12, and 15 recite that when the NAT firewall is detected then the calling user's respective global address is transmitted to the called user and the called user establishes the network session for the connection by transmitting to the calling user's respective global address. These steps are not disclosed by Buck et al. Moreover, Buck et al neither teaches nor suggests the dynamic reversal of the roles of the users' computers for establishing a direct (peer to peer) network session. Thus, claims 1, 3-7, 9-12, 14, 15, and 17 are allowable.

The rejection of claim 8 under 35 USC 103(a) as being unpatentable over Buck in view of AAPA is respectfully traversed. The statement in the final rejection that "it is obvious that a way to detect firewalls would be to recognize a mismatch in the global and local address of the equipment" fails to recognize that in prior art systems the global and local addresses are both known only to the firewall itself. As is well known in the art, the local address is not discoverable outside the NAT firewall. Therefore, a central server or an outside user could not detect a firewall because the only address they would see was the global address. Since there were not two addresses to compare as suggested in the final rejection, the prior art contains no suggestion of any method for detecting the presence of the NAT firewall. In the present invention, special steps must be taken in order to make the actual equipment address available to the central server so that the recited comparison can be made. For example, the application running on the protected user's computer which interacts

with the central server causes the actual equipment address to be sent as data during the registration process. Since nothing in either Buck or the AAPA suggests the recited address comparison for determining the presence of a NAT firewall, claim 8 is allowable.

In view of the foregoing amendment and remarks, claims 1, 3-12, 14, 15, and 17 are now in condition for allowance. Favorable action is respectfully solicited.

Respectfully submitted,



Mark L. Mollon
Attorney for Applicant(s)
Reg. No. 31,123

November 18, 2004
MacMillan, Sobanski & Todd, LLC
One Maritime Plaza, Fourth Floor
720 Water Street
Toledo, Ohio 43604
(734) 542-0900
(734) 542-9569 (fax)